REMARKS

Claims 1-23 are pending in this application.
Claims 1-17 and 19-23 are rejected.
Claim 18 is allowed.

The office action dated May 31, 2005 indicates that claim 18 contains allowable subject matter because the art made of record does not teach or suggest a printer for receiving an encrypted token from a remote site, using decryption key to decrypt the token, and sending the decrypted token to the remote site.

Claim 18 has been amended, but still recites these features. Features regarding document handling have been moved from claim 18 to new claim 24. Amended claim 18 and its dependent claim 24 should be allowed.

New claims 25-29 also recite the allowable subject matter. Therefore, new claims 25-29 should be allowed.

The office action indicates that base claim 12 is rejected under 35 USC §102(e) as being unpatentable over Debry U.S. Patent No. 6,385,728. The office action also indicates that base claims 1 and 19 are rejected under 35 USC §103(a) as being unpatentable over Debry in view of Mandelbaum U.S. Patent No. 5,552,897; and that base claim 11 is rejected under 35 USC §103(a) as being unpatentable over Debry in view of Mandelbaum, Furman U.S. Patent No. 5,483,653 and Boyle U.S. Patent No. 6,738,901.

The rejections of base claims 1, 11 and 19 are respectfully traversed (claim 1 has been amended for clarity). The rejection of base claim 12 is rendered moot

PAGE 11/15 * RCVD AT 7/20/2005 8:55:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-42

by the amendments above.

Debry discloses a document distribution system including a document source (file server), a user (client), and a print server. In the method of Figure 1, the user sends a request to the document source, and the document source creates a will-call certificate and sends the certificate to the user. The will-call certificate can include printer identification. Thus, the document source specifies the printer that will print the document.

The user receives the will-call certificate, includes it in a printer request, and sends the print request to the print server. The print server then sends the will-call certificate to the document source, along with its digital certificate. The document source uses the will-call and server certificates to verify the authenticity of the printer sever. If the print server is authenticated, a requested document is sent to the print server.

In the method of Figure 4, the end user is authenticated before a document is transmitted. Authentication is performed between the end user and the printer (col. 9, lines 16-27). Once the end user has been authenticated, the printer sends a print request, will-call certificate and digital certificate to the document source (col. 9, lines 36-40).

The digital certificate is "created by a process that enables a printer's manufacturer to build a secret key into the printer during manufacturing" (col. 10, lines 46-51). The key is recorded in a database maintained by a certificate authority.

In the method of Figure 5, the end user specifies the printer that will print the document. The end user obtains the printer's public key from the printer, and

PAGE 12/15 * RCVD AT 7/20/2005 8:55:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-42

sends the public key to the document source. The end user also sends (to the document source) information necessary to authenticate the printer. The document source creates a will-call certificate and sends it to the user. The user sends the will-call certificate and the publisher's URL to the print server. The print server then gets an encrypted document from the publisher.

In all three methods of Debry's methods, the will call certificate is handled by the end user. In all three of Debry's methods, the identity of the printer is fixed.

Claim 12

Claim 12 has been amended to recite a printer that establishes its printer identity directly with a server. Debry does not teach or suggest this feature. In all three methods of Debry's methods, a will call certificate is handled by the end user.

Claims 1 and 19

Debry does not teach or suggest changing the identity of a printer. Debry does not teach or suggest the use of a smart card to establish a printer identity with the document source. Debry does not teach or suggest a printer having no identity prior to using a smart card.

Although Mandelbaum discloses the use of a smart card in combination with a printer (e.g., fax machine), the smart card is not used to establish an identity of the printer. Mandelbaum discloses fax machine that receives an encrypted transmission. A recipient inserts a smart card into the fax machine, and the smart card decrypts the transmission (see col. 5, lines 33+). The transmission may be encrypted with recipient's public key and decrypted with the recipient's private key. The private key is stored in the smart card.

PAGE 13/15 * RCVD AT 7/20/2005 8:55:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-42

The document source sends an encrypted file to the fax machine, regardless of whether a smart card is inserted in the fax machine. Mandelbaum's system does not prevent the fax machine from receiving the encrypted document, even if the fax machine is not secure. Mandelbaum is not concerned with identifying the fax machine: the identity of the fax machine is tied to a phone number. The smart card is simply used as a decryption engine. If the recipient is not intended, presumably he will not have the correct smart card and, therefore, will not be able to decrypt the transmission.

Thus, Mandelbaum does not offer reason, incentive or motivation to modify Debry's system to use a smart card to establish a printer identity with a server. Therefore, base claims 1 and 19, and their dependent claims should be allowed over the combination of Debry and Mandelbaum.

Claim 11

The rejection of claim 11 is respectfully traversed. Claim 11 recites using a printer to indicate status of the printing so that a server can charge for copies that were actually printed, wherein the printer sends back a status acknowledgement to the server. The office action contends that Furman shows a status screen at col. 4, lines 20-24, and that Boyles (at col. 9, lines 18-21) teaches a network printer that registers a cost with a server for every copy that is printed.

However, Furman does not show a status screen at col. 4, lines 20-24. The passage simply states that a user can determine the status of a print job by making a request via a print server terminal or workstation (a server window can be used to give the user feedback that the print job is completed). Even if this passage did show a status screen, the status screen would not allow the server to charge for copies that were actually printed. As for Boyles, the passage at column 9, lines 18-21 does not teach a network printer that registers a cost with a server for every copy printed. Boyles simply states that a registered user's cash account

PAGE 14/15 * RCVD AT 7/20/2005 8:55:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-42

will be decremented whenever copies are made, purchases are made over the Internet, etc. These activities are all resident within a server, and, therefore, don't require information from a printer.

New claim 30

New claim 30 recites a printer including means for using at least one decryption key to establish a printer identity at the time of document distribution, the printer not having the identity prior to the document distribution. Debry, in contrast, discloses a printer having its identity determined at the time of manufacture.

New claim 31

New claim 31 recites a server that is programmed to wait for a printer to establish its identity within a timeout period and, if the identity is so established, to send at least one encrypted document to the printer after a document order has been placed, and to cancel the order if the identity is not established within the timeout period. This feature adds to the security of the system of claim 12.

The examiner is respectfully requested to withdraw the rejections of claims 1-17 and 19-23. The examiner is encouraged to contact applicants' attorney Hugh Gortler to discuss any issues that might remain.

PAGE 15/15 * RCVD AT 7/20/2005 8:55:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-42